



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/783,275	02/20/2004	Adrian M. Marinescu	MSFT122154	7623

26389 7590 10/18/2007
CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE, WA 98101-2347

EXAMINER

SONG, HOSUK

ART UNIT	PAPER NUMBER
----------	--------------

2135

MAIL DATE	DELIVERY MODE
-----------	---------------

10/18/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/783,275

Applicant(s)

MARINESCU, ADRIAN M.

Examiner

HOSUK SONG

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 February 2004.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-35 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-4, 6, 12-18, 20 and 26-35 is/are rejected.
- 7) ☒ Claim(s) 5, 7-11, 19 and 21-25 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 20 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 10783275.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- ☐ Notice of Informal Patent Application
- ☐ Other: _____

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4,6,12-18,20,26-35 are rejected under 35 U.S.C. 102(e) as being anticipated by Zisowski(US 7,228,434).

Claim 1: Zisowski disclose selecting evaluation calls made by the executable to the interface of an operating system and loading stubs into a virtual address, the stubs in (col.8,lines 3-13). Zisowski disclose mirroring the calls made to the interface of an operating system and determining a behavior signature for the selected calls in (fig.1 and col.8,lines 57-67). Zisowski disclose executing the selected calls inside of a virtual operating environment using the loaded stubs dynamically libraries and determining the behavior signatures resulting from execution of selected calls inside of a virtual operating environment in (fig.1 and col.3, lines 44-47;col.8,lines 27-56).

Claims 2-6: Zisowski disclose calls selected for evaluation are a subset of calls made by the executable to the interface of an operating system in (fig.1, col.8,lines 3-14).

Claims 12-14: Zisowski disclose loading subs is initiated by an event generated by the virtual operating environment in (col.8,lines 3-13).

Claim 15: Zisowski disclose selecting evaluation calls made by the executable to the interface of an operating system and loading stubs into a virtual address space, the stubs in (col.8,lines 3-13). Zisowski disclose mirroring the calls made to the interface of an operating system and determining a behavior signature for the selected calls in (fig.1 and col.8,lines 57-67). Zisowski disclose executing the

Art Unit: 2135

selected calls inside of a virtual operating environment using the loaded stubs dynamically libraries and determining the behavior signatures resulting from execution of selected calls inside of a virtual operating environment in (fig.1 and col.3, lines 44-47;col.8,lines 27-56).

Claims 16-20: Zisowski disclose calls selected for evaluation are a subset of calls made by the executable to the interface of an operating system in (fig.1, col.8,lines 3-14).

Claims 26-28: Zisowski disclose loading subs is initiated by an event generated by the virtual operating environment in (col.8,lines 3-13).

Claim 29: Zisowski disclose a manager for obtaining an executable and directing calls that are potentially indicative of malware to an simulator and a loader for making stubs related to calls that are potentially indicative of malware available to the simulator in (col.7,lines 55-67; col.8,lines 3-12 and fig.1). Zisowski disclose a simulator for executing calls received from manager, execution completed using stubs obtained from loader and storage for storing the results of simulator or executing calls received from manager in (fig.1 and col.3, lines 44-47;col.8,lines 27-56).

Claim 30: Zisowski disclose simulator receives and recalls data during the execution of calls received from manager in (fig.1).

Claims 31-32: Zisowski disclose a comparator for comparing calls contained in executable with calls that are indicative of malware in (col.8,lines 35-43).

Claims 33-35: Zisowski disclose an interface operative to accept an executable and identify calls that are potentially indicative of malware in (col.8,lines 35-43). Zisowski disclose a ser of abbreviated application program interface handlers that mirror a set of fully-implemented application program interface handlers and an input/output emulator operative to simulate computer devices that accept input or generate output in (fig.1).Zisowski disclose a virtual address space for the storage of stubs, the stubs linked to calls made by executable and a memory management unit for mapping locations in memory to a virtual address space in (fig.1 and col.3, lines 44-47;col.8,lines 27-56).

Art Unit: 2135

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 29,33 are directed to a software system. The claimed invention is an abstract idea or non-functional descriptive material (data or information) with no practical information. The claimed invention is directed to non-statutory subject matter. The 101 issue can be overcome by claiming a hardware or performing steps in a hardware.

Claims 30-32,34-35 do more than provides specific about the data or information ad claims 29,33 then claims are also rejected.

Allowable Subject Matter

Claims 5,7-11,19,21-25 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

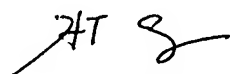
USPTO Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HOSUK SONG whose telephone number is 5712723857. The examiner can normally be reached on mon-fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, KIM VU can be reached on 5712723859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2135

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.


HOSUK SONG
PRIMARY EXAMINER